# On the Security Vulnerabilities of a Hash Based Strong Password Authentication Scheme

**Manoj Kumar**
Department of Mathematics
R. K. College Shamli-Muzaffarnagar, U.P.-India - 247776
E-mail: yamu_balyan@yahoo.co.in

## Abstract

*User authentication is an essential task for network security. To serve this purpose,in the past years, several strong password authentication schemes have been proposed, but none of them probably withstand to known security threats. In 2004, W. C. Ku proposed a new hash based strong password authentication scheme and claimed that the proposed scheme withstands to replay, password fie compromise, denial of service and insider attack. This paper analyzes W. C. Ku's scheme and found that the proposed scheme does not support mutual authentication, session key generation phase for secure communication. In addition, in W. C. Ku's scheme, the user is not free to change his password. However, in this paper, we show that W. C. Ku's scheme is still vulnerable to insider, man in the middle, password guessing, replay, impersonation, stolen verifier and denial of service attacks.*

***Keywords**: Login, server, access system, mutual authentication, session key, network security.*

## 1. Introduction

The rising and flourishing development of client server network provides access rights to a valid client or online facilities to their clients in order to managing their daily work. This client-server network consists of an authentication server (*AS*) and a number of clients willing to exchange online information with the server. On the one end, the *AS* always has own secret key, which is never exchanged with a client, while at the other end, the client has a secret piece of information, named as password. In order to ensure high level of security for this client server system, a password based authentication protocol is widely used. In client-server system, password-based authentication is a way that can ensure the client has authorization to access the server. Actually, a password authentication protocol uses a two-way handshake to perform authentication. Once the communication link is established, the client sends a username and password to the server. The server uses its own authentication scheme and user database to authenticate the user and if the authentication is valid, the server sends an acknowledgment to the client and a user gets access to the system. In conventional password authentication schemes,the *AS* has a record of the clients's name and related passwords database. The client usually exchanges either its password or a variation of it (e.g., encrypted form) with the server. By receiving the password, the server compares the received password with the one stored in the clients's name and related passwords database, to deny or grant the client to access to the system. In other words, client has no chance of getting the access rights to the server unless he/she exchanges the valid password or its variation across the network. The drawback of this conventional method is that during the authentication process the client's password may be exposed to an adversary or a man-in-the-middle. Thus,a clear-text password exchanged in password based authentication is not a secure form of authentication, because the user's passwords are passed over the link in plain form. In order to provide the security to the exchanged password during the authentication process,a number of techniques have been developed to securely exchange the password over the network [3, 4, 5, 6, 8, 9, 10, 11, 13].

### 1.1 Our Contribution

In 2004,W. C. Ku [13] proposed a hash-based strong-password authentication scheme. According to W. C. Ku, the proposed scheme withstands to the several attacks, including replay, password file compromise, denial-of-service, and insider attack. This paper analyzes that W. C. Ku's scheme does not satisfy some essential security requirements. The proposed scheme only has registration and login phase. W. C. Ku's scheme does not support session key generation and mutual authentication phase for secure communication. In addition, in W. C. Ku's scheme, the remote user is not free to change his password. The lack of session key generation and mutual authentication phases in W. C. Ku's scheme leads to other serious security vulnerabilities. The purpose of this paper is to show that W. C. Ku's scheme is vulnerable to insider attack, parallel session attack, password guessing attack, man in the middle attack, stolen-verifier attack, impersonation attack, reflection attack and denial-of-service attack. On the other side, W. C. Ku's scheme also does not satisfy the essential security attributes [4, 9].

### 1.2 Organization

The remainder of this paper is organized as follows. Section 2 is about the notations. Section 3 reviews the W. C. Ku's scheme. The security vulnerabilities and attributes of W. C. Ku's scheme are analyzed in section 4. Finally, comes to conclusion in the section 5.

## 2 Notations

- *U* denotes the User.
- *S* denotes the Server.
- *A* denotes the Adversary.
- *h* denotes a cryptographic hash function.
- *h*(*m*) means the message *m* is hashed once, while $h_2(m)$ means *m* is hashed twice, *i.e.* $h_2(m) = h(h(m))$.
- *r* denotes a random nonce.
- *N* denotes an integer starting from 1 since *U*'s initial registration.
- *PW* denotes the strong password of *U*.
- $X_s$ denotes the secret-key of *S*.
- *T* denotes the most recent time, when *U* initially registered or re-registered at *S*.
- $\bigoplus$ denotes the bitwise XOR operation.
- || denotes the concatenation.
- The expression $A \rightarrow B : X$ means *A* sends the message *X* to *B* via an insecure channel.
- The expression $A \Leftrightarrow B : X$ means *A* sends the message *X* to *B* via a secure channel.

## 3 Review of W. C. Ku's Scheme

This section reviews W. C. Ku's scheme [13]. W. C. Ku's scheme has two phase: the registration phase and the login phase.

### 3.1 Registration Phase

This phase is invoked whenever *U* initially registers or re-registers to *S*.

1. *U* sends his registration request to *S*.

2. $S \rightarrow U : r, N, T$.
   *S* sets *T* as the currently value of the time. If this is *U*'s initial registration, *S* sets *N* = 1, otherwise *S* sets *N* = *N* + 1. Next, *S* sends *N* and *T* to *U*.

3. $U \Leftrightarrow S : h_2(S \parallel PW \parallel N \parallel T)$.

4. *S* computes the user storage key $K_U^{(T)}$ and the sealed verifier $sv^{(N)}$,as,

$$\begin{aligned} K_U^{(T)} &= h(U \parallel h(X_s \parallel T)) \\ sv^{(N)} &= h_2(S \parallel PW \parallel N \parallel T) \bigoplus K_U^{(T)}. \end{aligned}$$

5. *S* stores $sv^{(N)}$, *N* and *T* in the password file.

### 3.2 Login Phase

This phase is invoked whenever *U* logins to *S*.

1. *U* sends his login request to *S*.

2. $S \rightarrow U : r, N, T$

3. $U \rightarrow S : c_1, c_2, c_3$. where

$$\begin{aligned} c_1 &= h_2(S \parallel PW \parallel N \parallel T) \bigoplus h(S \parallel PW \parallel N \parallel T), \\ c_2 &= h(S \parallel PW \parallel N \parallel T) \bigoplus h_2(S \parallel PW \parallel N+1 \parallel T), \\ c_3 &= h(h_2(S \parallel PW \parallel N+1 \parallel T) \parallel r). \end{aligned}$$

4. S computes $K_U^{(T)} = h(U \parallel h(X_s \parallel T))$.

5. S derives $h_2(S \parallel PW \parallel N \parallel T) = sv^{(N)} \bigoplus K_U^{(T)}$.

6. *S* computes $u_1$ and $u_2$ ,as,

$$\begin{aligned} u_1 &= c_1 \bigoplus h_2(S \parallel PW \parallel N \parallel T) \\ &= h(S \parallel PW \parallel N \parallel T), \\ u_2 &= c_2 \bigoplus u_1 \\ &= h_2(S \parallel PW \parallel N+1 \parallel T). \end{aligned}$$

7. If the equalities $h(u_1) = h_2(S \parallel PW \parallel N \parallel T)$ and $h(u_2 \parallel r) = c_3$ hold, then *S* authenticates *U*, otherwise, *S* rejects *U*'s login request and terminates this session.

8. After a successful authentication, *S* computes a new sealed-verifier using $sv^{(N+1)} = u_2 \bigoplus K_U^{(T)} = h_2(S \parallel PW \parallel N \parallel T) \bigoplus K_U^{(T)}$, and replaces $sv^{(N)}$ with $sv^{(N+1)}$, and sets N = N + 1 for *U*'s next login. The value of *T* is unchanged.

# 4 Security Vulnerabilities and Attributes of W. C. Ku's Scheme

## 4.1 Man in the Middle Attack

To apply man in the middle attack (often abbreviated MITM) the attacker intercepts the communications/messages over the insecure network. For example, an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle. Man in the middle attacks are sometimes known as fire brigade attacks. The term derives from the bucket brigade method of putting out a fire by handing buckets of water from one person to another between a water source and the fire. The eavesdropper uses a program that appears to be the server to the client and appears to be the client to the server.In this way, the entire conversation is controlled by the attacker and the attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances the two original parties still appear to be communicating with each other. The attack may be used simply to gain access to the message or enable the attacker to modify the message before retransmitting it. A man-in-the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other. The following discussion proves that how an malicious user *A* can mount MITM attack on W. C. Ku's hash based strong password authentication scheme, whenever the user *U* sends his login request to *S*.

1. *U* sends his login request $L_U$ to *S*.
   Malicious user *A* intercept the login request $L_U$ and replace the login request $L_U$ with own valid login request $L_A$.

2. *A* sends his login request $L_A$ to *S*.

3. $S \rightarrow U : r, N, T$.
   Malicious user *A* intercept $r, N, T$ and replace these values with $r_A, N_A, T_A$

4. $A \rightarrow U : r_A, N_A, T_A$.

5. $U \rightarrow S : c_1, c_2, c_3$, where

$$\begin{aligned} c_1 &= h_2(S \parallel PW \parallel N \parallel T) \bigoplus h(S \parallel PW \parallel N \parallel T), \\ c_2 &= h(S \parallel PW \parallel N \parallel T) \bigoplus h_2(S \parallel PW \parallel N+1 \parallel T), \\ c_3 &= h(h_2(S \parallel PW \parallel N+1 \parallel T) \parallel r). \end{aligned}$$

   Malicious user *A* intercept $c_1, c_2, c_3$ and replace these values with $c_1^A, c_2^A, c_3^A$,where

$$\begin{aligned} c_1^A &= h_2(S \parallel PW_A \parallel N_A \parallel T_A) \bigoplus h(S \parallel PW_A \parallel N_A \parallel T_A), \\ c_2^A &= h(S \parallel PW_A \parallel N_A \parallel T_A) \bigoplus h_2(S \parallel PW_A \parallel N_A+1 \parallel T_A), \\ c_3^A &= h(h_2(S \parallel PW_A \parallel N_A+1 \parallel T_A) \parallel r_A). \end{aligned}$$

6. $A \rightarrow S : c_1^A, c_2^A, c_3^A$

7. S computes $K_A^{(T_A)} = h(A \parallel h(X_s \parallel T_A))$.

8. S derives $h_2(S \parallel PW_A \parallel N_A \parallel T_A) = sv^{(N_A)} \bigoplus K_A^{(T_A)}$.

9. *S* computes $u_1$ and $u_2$ ,as,

$$\begin{aligned} u_1 &= c_1^A \bigoplus h_2(S \parallel PW_A \parallel N_A \parallel T_A) \\ &= h(S \parallel PW_A \parallel N_A \parallel T_A), \\ u_2 &= c_2^A \bigoplus u_1 \\ &= h_2(S \parallel PW_A \parallel N_A+1 \parallel T_A). \end{aligned}$$

10. Obviously,the equalities $h(u_1) = h_2(S \parallel PW_A \parallel N_A \parallel T_A)$ and $h(u_2 \parallel r_A) = c_3^A$ hold, therefore *S* authenticates *A* in place of *U* and starts a session. In this way, the malicious user *A* records all the confidential communication.

### 4.2 Insider Attack

There are a variety of reasons for a possible insider attack in an organization's computer network. In most of the organizations, the access control settings for security-relevant objects do not reflect the organization's security policy. This malicious attack is planted by someone who has been entrusted with authorized access to the organization's computer network and also may have knowledge of its architecture therefore insider attack is the primary threat to computer networks of an organization. This allows the insider to browse through sensitive data, but they require such access in order to serve their function.Furthermore, as they have already user accounts and corporate e-mail addresses, they likely have access to company data. If the user *U* uses the same password to access other servers for convenience, the insider insider at server *S* can impersonate the user *U* to access other services. Thus, insider can also affect all components of organization's computer network and its security on behalf of user *U*. Since, the insider has a legitimate access to the organization's computer network, therefore he can create the following destructive attacks of his choice on behalf of user *U*. If, we observe W. C. Ku's hash based strong password authentication scheme,then it is clear that the insider at server *S* is in possession of the following information.

- Password file of user *U* containing the current *N, T*.
- The value $h_2(S \parallel PW \parallel N \parallel T)$.
- All past records about the values *r, N, T*.
- The login request records $c_1, c_2, c_3$.
- The verification records $u_1 = h(S \parallel PW \parallel N \parallel T)$ and $u_2 = h_2(S \parallel PW \parallel N+1 \parallel T)$.

Now, by manipulating these recorded information, the insider at server can mount an attack of his choice without knowing the related password of a valid user. The insider will be able to mount stolen verifier attack, denial of service attack,password guessing attack,impersonation attack, replay attack etc. Thus, in W. C. Ku's scheme, the insider is a strong antagonist. Beside the above vulnerabilities, the insider will be able to do the following malicious activity.

1. Insider can steal valuable propriety information of the company's network.
2. Insider can plant trojan horses or browse through the file system.
3. Insider can affect availability by overloading the system's processing or storage capacity or by causing the system to crash.

### 4.3 Off-line Password Guessing Attack

To recover one or more plaintext passwords from hashed password is known as password guessing attack. Off-line password guessing attack is the process of recovering password from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Since, in W. C. Ku's scheme, the user is not free to change his password, therefore an adversary can set a off-line password guessing attack. This section shows that W. C. Ku's hash based strong password authentication scheme [13] cannot withstand password guessing attack.For the success of password guessing attack, an adversary will perform the following operations.The adversary intercepts the login phase and records the following insecure phase.

$S \rightarrow U : r, N, T$

$U \rightarrow S : c_1, c_2, c_3$, where

$$\begin{aligned} c_1 &= h_2(S \parallel PW \parallel N \parallel T) \bigoplus h(S \parallel PW \parallel N \parallel T), \\ c_2 &= h(S \parallel PW \parallel N \parallel T) \bigoplus h_2(S \parallel PW \parallel N+1 \parallel T), \\ c_3 &= h(h_2(S \parallel PW \parallel N+1 \parallel T) \parallel r). \end{aligned}$$

After the above setting,to guess a valid password via $c_1$, the adversary performs the following steps.

1. Set the value $N, T$ for the server *S*.

2. Guess a password $PW_i$.
3. Computes $c_i = h_2(S \parallel PW_i \parallel N \parallel T) \bigoplus h(S \parallel PW_i \parallel N \parallel T)$
4. Check, whether $c_i = c_1$, if it holds, it means the adversary has managed to guess a valid password, otherwise go to step-2 and set a different password $PW_i$.

In the similar way, the adversary can guess a valid password via $c_2$ or $c_3$.

### 4.4 Attributes of W.C.Ku's Scheme

An ideal password authentication scheme should achieve some essential security attributes [4, 9], while W. C. Ku's scheme does not satisfy the following attributes. In W.C.Ku's Scheme,

1. The passwords or verification tables are stored in the system.
2. The passwords can not be changed freely by the users.
3. The passwords can be guessed by the insider at the server.
4. Some information are transmitted in plain text over the insecure network, which are responsible for security vulnerabilities.
5. The length of a password is nor specified, while the length of the password must be appropriate for memorization.
6. The efficiency and practical abilities are not described.
7. There is no unauthorized login detection, when a user inputs a wrong password. The user can enter his password multiple times, it means there is a possibility of online password guessing attack.
8. No session key is generated during the password authentication process to provide confidentiality of communication.
9. The login ID is not dynamically changed for each login session to avoid partial information leakage about the user's login message.
10. The server is not forward protected. The proposed scheme is completely insecure if the secret key of the server is leaked out or stolen.

## 5 Conclusion

This paper analyzes W. C. Ku's scheme and found that the proposed scheme neither provide mutual authentication between the user and server, nor establish a common session key to provide message confidentiality. In W. C. Ku's scheme, the user is not free to change his password. Due to these deficiencies, W. C. Ku's scheme is vulnerable to insider attack, stolen verifier attack,denial of service attack, impersonation attack, MITM attack,off-line password guessing attack etc. However, W. C. Ku's scheme does not support the essential security attributes.

## References

[1] Chang C. C. and Hwang K. F., 2003. Some forgery attack on a remote user authentication scheme using smart cards. *Informatics*, 14-3, pp. 189 - 294.

[2] Chen, C.M. and Ku, W.C., 2002. Stolen-verifier attack on two new strong-password authentication protocols. *IEICE Transactions on Communications*, E85-B (11),pp. 2519-2521.

[3] Han C. H. , Shih W.K., 2009. Weaknesses and improvements of the Yoon Ryu Yoo remote user authentication scheme using smart cards, *Computer Communications*, Volume 32- 4,pp. 649-652.

[4] IEEE P1363.2-D13, 2004. Standard Specifications for Password-based Public Key Cryptographic Techniques. *IEEE P1363 working group*.

[5] Jia Y. L. An-Min Zhou, Min-Xu Gao, 2008. A new mutual authentication scheme based on nonce and smart cards. *Computer Communications*. Volume 31, Issue 10, , pp. 2205-2209.

[6] Lamport L., 1981. Password authentication with insecure communication. *Communication of the ACM*, 24, 11: pp. 770-772.

[7] Mitchell C. J. and Chen l.,1996. Comments on the S/KEY user authentication scheme. *ACM Operating System Review*, vol. 30, No. 4, pp. 12-16.

[8] Shen Z. H., 2008. A new modified remote user authentication scheme using smart cards.*Applied Mathematics*,Volume 23-3, 371-376.

[9] Tsai C. S., Lee C. C.and Hwang M. S., 2006.Password Authentication Schemes: Current Status and Key Issues. *International Journal of Network Security*, Vol.3, No.2, pp. 101 115.

[10] Wang Y.Y., Liu J. Y., Xiao F. and Dan J., 2009. A more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications* ,Volume 32, Issue 4, P.P. 583-585.

[11] Yen S. M. and Liao K. H., 1997. Shared authentication token secure against replay and weak key attack. *Information Processing Letters*, 78-80.

[12] W. C. Ku, H. C. Tsai, and S. M. Chen, Two simple attacks on Lin-Shen-Hwang's strong-password authentication protocol," *ACM Operating System Re view*, vol. 37, no. 4, pp. 26-31, Oct 2003.

[13] W. C. Ku, A hash-based strong-password authen tication scheme without using smart cards," *ACM Operating System Review*, vol. 38, no. 1, pp. 29-34, Jan 2004.

**Manoj Kumar** received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography(Applied Algebra), from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi- India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to Feb 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. - INDIA from March 2001 to Oct 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. - INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is working in Department of Mathematics, R. K. College Shamli- Muzaffarnagar- U.P. - INDIA-247776. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as a reviewer for some International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The computer networks, computer and security, The Computer Journal. He is also working as a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He has published his research works at national and international level. His current research interests include Cryptography and Applied Mathematics.